REMARKS

Introduction

This Reply is in response to the Office Action of March 28, 2008. Reconsideration of this application in view of the following remarks is respectfully requested.

Claims 12-15

In the Office Action, claims 12-15 were rejected under 35 U.S.C. 103(a) as being unpatentable over Roesch et al. U.S. Patent No. 7,240,368 in view of Shukla U.S. PG-PUB 2002/0042875. These rejections are respectfully traversed.

Applicant's invention relates to a method for preventing intrusions to a computer system. Claim 12 is directed to a method that uses a virtual proxy to analyze intercepted data packets in order to detect intrusions. In the Office Action, the Examiner suggested that Roesch contains many of the elements of claim 12, including using a network-based appliance to intercept data packets, deciding whether to forward the intercepted packets or whether to route the intercepted packets to a virtual proxy, performing TCP or UDP processing on the intercepted packets to a virtual proxy, and using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions. The Examiner suggested

that Roesch's intrusion and misuse deterrence system (IMDS) is analogous to applicant's virtual proxy.

The Examiner also acknowledged that Roesch fails to teach using a virtual proxy to direct a transport layer to modify packets. To make up for this shortcoming in Roesch, the Examiner suggested that Shukla discloses modifying packets at the transport layer, and that it would have been obvious to one of ordinary skill in the art to modify the transport layer to "protect the packet from NATs."

However it is applicant's view that not all of the elements attributed to Roesch are in fact contained in Roesch. Shukla fails to make up for these deficiencies in Roesch.

Roesch describes a system that uses IMDS 85 to increase the security of a computer network. Roesch's IMDS 85 is a server on a network that simulates a synthetic network, and thereby draws away intruders from the real network. The real network in Roesch is represented as network 40 in Roesch's FIG 2, while Roesch's synthetic network is shown as network 60 in Roesch's FIG. 2. Incoming packets addressed to real network 40 are never received by IMDS 85, and IMDS 85 never analyzes the packets it receives because these packets are assumed to be associated with intruders.

All packets that attempt to access services associated with the synthetic network ("façade services") are assumed to

originate from intruders, as there are no legitimate users of the synthetic network. (Roesch 7:63-7:66) Intruders can thus be identified.

The system described in Roesch is a passive system that is used to maintain logs 84 of traffic that is assumed to represent intrusions. The IMDS "passively detects network intruders in a manner that adds little overhead to a computer network." (Roesch 1:63-1:64) Each packet that is routed to the IMDS is assumed to originate from an intruder, whereupon IMDS 85 "identifies the source of the packet and notifies a system administrator of the presence of a network intruder." (Roesch 3:03-3:05) The IMDS is capable of automatically sending emails or notifying network entities, but never needs to analyze incoming traffic, because all packets that attempt to access facade services maintained by the IMDS are assumed to be intrusion traffic.

The applicant's virtual proxy, in contrast, is not such a passive system. The virtual proxy of claim 12 analyzes packets to detect whether or not they are intrusions. The IMDS of Roesch assumes that all received packets originate from intruders so Roesch's IMDS does not analyze packets, let alone does Roesch's IMDS analyze packets to detect intrusions as required by claim 12.

The feature of claim 12 pertaining to "using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions" is simply not shown or suggested by Roesch. Moreover, this element of claim 12 has been expanded to read: "using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions using a processing engine having at least one processing procedure that detects intrusions." (See e.g. applicant's FIG. 1.) This makes the distinction from Roesch even clearer. Roesch's IMDS does not determine whether packets are intrusions using a processing procedure in a processing engine, as all packets are assumed to be intrusions. Shukla, which was cited as showing modification to packets, does nothing to make up for these deficiencies in Roesch.

Claim 12 is therefore patentable over Roesch and Shukla. Dependent claims 13-15 are patentable because they depend from claim 12.

Conclusion

The foregoing demonstrates that claims 12-15 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

Respectfully submitted,

Date: September 11, 2008

/G. Victor Treyz/
G. Victor Treyz
Reg. No. 36,294
Attorney for Applicant
Customer No. 36532